AICPA®
Member Insurance Programs

A CPA firm's guide to cyberliability basics

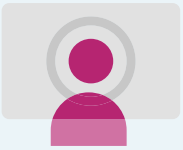
Brought to you by

AON

Underwritten by

CNA

A CPA firm's guide to cyberliability basics



The threat of cybercrime is vast and growing. In 2022, the Federal Bureau of Investigation's Internet Crime Record reported that organizations had lost **$10.3 billion** that year due to cybercrime across the globe, an almost 50% increase from the prior year.[1]

The average cost of a data breach is increasing as well, reaching an all-time high of $4.45 million in 2022, an increase of over 15% since 2020.[2]

Cybercrimes cost companies billions worldwide and show no sign of stopping.

Is your firm doing what it can to help protect against data breaches?

In this eBook, we will review the current state of cybercrime, how to improve your cybersecurity, and help reduce your firm's risk.

Table of contents

Data security incidents 101

Before you can help protect yourself from cybercrimes, you need to know what to look out for.

What is a data security incident?

This is a security event that threatens the integrity, confidentiality, or availability of data. An incident can result in a breach which is the confirmed unauthorized disclosure of data.

Information targeted

Depending on the goals of the cybercriminal, they may target one or more of the following:

- **Protected Health Information (PHI)** Includes, but is not limited to, information on demographics, medical history, mental health conditions, insurance details, lab work or medical testing
- **Personally Identifiable Information (PII)** Includes, but is not limited to, details about a person's identity including legal name, address, email, social security, date of birth, credit card details, or identification numbers
- **Trade secrets** Private company information that outside entities could profit from
- **Other confidential information**

Attack vectors

No two cyber attacks are the same. Some of the top causes of data breaches include:

- **Social engineering/phishing**
- **Accidental data leak or exposure**
- **Cloud misconfiguration**
- **Stolen/compromised credentials**
- **Physical security compromise**
- **Lost or stolen device**
- **Malicious insider**
- **Business email compromise**

Cyber breach repercussions

A data breach could lead to identity theft or a violation of industry regulation or applicable law and may also lead to:

- **Fines**
- **Claims/litigation**
- **Civil damages**
- **Damage to reputation**
- **Business interruption**
- **Loss of the trust of your clients**

Spotlight on social engineering

2

Social engineering is one of the most common causes of data security incidents. This sneaky way of accessing information is achieved through:

Psychological manipulation

Tricking people into making security mistakes or giving away sensitive information

Capitalizing on human error, rather than a software system vulnerability

Baiting

Lures people into a trap that allows unauthorized network access to either steal personal information or introduce malware.

Scareware

Bombards a victim with false alarms and fictitious threats.

Pretexting

Attacker obtains information through a series of cleverly crafted lies.

Phishing

Email and text message campaigns aimed at creating a sense of urgency, curiosity, or fear.

Spear Phishing

More targeted than a standard phishing scam. Messages are tailored based on the characteristics, job position, and contacts belonging to the victim.

Social engineering relies on a mistake from an individual, rather than a technical error, but that doesn't mean it's less dangerous. While there are many types of data security incidents, they can almost always be attributed to one thing: a vulnerability or gap in a firm's security. In other words, a security weakness.

Could your firm be vulnerable to a data incident?

The sad truth is that any size firm can fall prey to a cyberattack, and the consequences can be catastrophic. 60% of small companies go out of business within six months of falling victim to a data breach or cyberattack.[3] Accounting firms are a prime target for hackers because:

- **CPAs are aggregators of data –** both financial and personal
- **CPAs also may have access to client funds and other liquid assets**
- **CPAs may be perceived as having weak data security controls**

It could happen to you

As we have shown, there are many methods cybercriminals can use to infiltrate a firm. Curious about what this could look like at your firm?

3

A small ransom demand leads to big expenses!

Scenario: A CPA firm was unaware that its network had gaps in cyber security.

The attack: As a result of a quick click on an unremarkable, but malicious, link, hackers were able to gain a foothold into the firm's system. The bad actors locked up the firm's entire network and demanded $1,000 to restore access. The firm was shocked by the attack but relieved that such a small ransom was demanded. That relief was short lived.

The consequences: The firm paid the ransom, and access was restored. However, the hacker left a backdoor as a parting gift and attacked again, this time demanding $1 million. Faced with looming client and payroll deadlines, the firm spent over $100,000 for forensic investigation and remediation, data recovery, client notification, and crisis management.

Theis scenario is frightening, but luckily there are steps you can take to help make your firm more secure.

Preventative measures your CPA firm can take to help reduce risk

4

Now that you understand the risks that come with cyberattacks, we will explore preventative measures you can take to help protect your firm.

Risk mitigation checklist

Have you taken any of these basic steps already? If not, work to implement them as soon as possible. There's no telling when a cyberattack will take place so it pays to be prepared.

Administrative safeguards

- [ ] Reassess safeguards currently in place to maintain data security
- [ ] Train and re-train employees concerning your firm's security program, practices, and procedures. Periodically test their understanding
- [ ] Select service providers capable of maintaining appropriate safeguards, and require those safeguards by contract
- [ ] Adjust your security program considering business changes or new circumstances

Technical safeguards

- [ ] Assess risks in network and software design
- [ ] Assess risks in information processing, transmission, and storage
- [ ] Securely dispose of private information within a reasonable amount of time after it is no longer required by the firm's record retention policy
- [ ] Implement security software and controls to help detect, prevent, and respond to attacks or system failures
- [ ] Create an incident response plan, and regularly test its effectiveness through simulations

Seek a third-party data expert's guidance to:

- [ ] Help identify your firm's vulnerabilities
- [ ] Educate you on potential solutions to help protect your data
- [ ] Help conduct regular drills that test your firm's response in case of an attack
- [ ] Provide the technical knowledge necessary to conduct penetration testing and implement scanning software
- [ ] Train staff on preventative measures to take to help avoid a security incident

What to do if there has been an incident?

5

When you suspect you've had a security incident, it's important to act fast. Here is a quick overview on what you can do should there be a cyberattack.

1 Lock it down!

- **Contain the damage and UNPLUG from the firm's network**
- **Disconnect servers, computers, and devices from the internet**
- **Disable any remote access**
- **Check firewalls**
- **Change all passwords**
- **Do not wipe systems. Doing so will destroy information needed to determine if a breach has occurred.**

2 Contact your cyber insurer

You should contact your insurer BEFORE you let your in-house IT staff work to fix the issue because:

- **There's likely a "weakness" in your system**
- **Your IT staff most likely does not have not have the requisite skills to investigate the incident**
- **You can rely on your insurer as well as legal counsel and data security experts for advice and recommendations on how to plug the "weakness"**

3 Remediate

- **Conduct forensics to determine the cause of the incident and whether data has been exposed**
- **Recover data and determine notification obligations**
- **Fix any gaps you discover in your cybersecurity risk management protocols**

Cyberliability insurance: manage your risk

6

Does your firm have cyber liability insurance?
Here are the basics on this valuable insurance coverage:

What is cyberliability insurance?

Cyberliability insurance is designed to address your firm's response to a data breach involving sensitive customer information, such as, but not limited to:

- **Social security numbers**
- **Credit card numbers**
- **Account numbers**
- **Driver's license numbers**
- **Health records**

What should you look for in a policy?

Check your existing coverage and consult with your agent/broker to determine if you are adequately covered for:

Cyberliability coverage*

- **Privacy event expense coverage** Covers expenses associated with complying with statutes/regulations, including notification costs and credit monitoring
- **Network damage claim coverage** Covers claims brought by third parties, such as vendors, merchants, service providers, and others, whose computer networks and information may have been damaged
- **Extortion coverage** Subject to consent, provides coverage for reasonable and necessary expenses to directly respond to an extortion threat to launch an attack on, or otherwise disrupt, your network
- **First party** Covers reimbursement for lost business income that the firm would have earned, and extra expenses incurred while operations were substantially interrupted
- **Regulatory proceedings/fines** Covers attorneys' fees and other reasonable costs in responding to regulatory proceedings and associated regulatory fines

Crime coverage*

- **Limit risk exposure** Limit exposure against risk of loss of or damage to certain types of property resulting from fraud schemes like social engineering and ransomware scams
- **Computer fraud** Covers loss resulting from use of a computer to fraudulently transfer covered property through unauthorized and intentional use of corrupt code by outside party
- **Funds transfer fraud** Covers loss resulting from a fraudulent instruction directing a financial institution to transfer, pay or deliver money or securities
- **Social engineering fraud** Covers loss resulting from the intentional misleading of an employee through use of a communication by a party, who is not, but purports to be the insured, an employee, or a pre-existing client or a vendor

*Coverage is subject to a policy's terms and conditions.

In conclusion

Protecting your firm from cybercrime is more important than ever. To learn more about how to help protect your firm refer to the AICPA Member Insurance Programs page.

For a complimentary consultation

Please call 1-800-221-3023
Monday through Friday, 8 a.m. to 6 p.m. ET, to speak with AICPA Risk Advisor.
To review our insurance portfolio and risk mitigation resources visit cpai.com.

Additional AICPA Member Insurance Programs cybersecurity resources

- Don't get victimized by a cybercriminal
- Four steps to better cybersecurity
- Cyberliability: managing evolving exposures
- A cyberattack could spell disaster for your CPA firm
- Doing business in the cloud? Carry an umbrella
- Professional Liability Risks Related to Cloud Computing
- Cybersecurity risk: Constant vigilence required
- Controlling Your Data

1 https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
2 https://www.ibm.com/reports/data-breach
3 https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

AICPA® Member Insurance Programs

A CPA firm's guide to cyber liability basics

Brought to you by AON

Underwritten by CNA

Note: The information contained in this guide is designed to provide an overview to starting a business, and is not intended to address all issues or provide individual advice. For professional information and advice, be sure to contact your attorney, financial planner, retirement counselor, or others for guidance

All descriptions, summaries or highlights of coverage are for general informational purposes only and do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy.

Aon Insurance Services is the brand name for the brokerage and program administration operations of Affinity Insurance Services, Inc. (TX 13695), (AR 100106022); in CA and MN, AIS Affinity Insurance Agency, Inc. (CA 0795465); in OK, AIS Affinity Insurance Services Inc.; in CA, Aon Affinity Insurance Services, Inc. (CA 0G94493), Aon Direct Insurance Administrator and Berkely Insurance Agency; and in NY, AIS Affinity Insurance Agency.

This ebook provides information, rather than advice or opinion. It is accurate to the best of the author's knowledge as of the ebook date. This ebook should not be viewed as a substitute for recommendations of a retained professional. Such consultation is recommended in applying this material in any particular factual situations.

Examples are for illustrative purposes only and not intended to establish any standards of care, serve as legal advice, or acknowledge any given factual situation is covered under any CNA insurance policy. The relevant insurance policy provides actual terms, coverages, amounts, conditions, and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice.